Listing of claims:

Claims 1–34 (canceled).

Claim 35 (previously presented) A method for authenticating a payment transaction over a network, comprising:

storing a public key associated with a public key infrastructure (PKI) key pair in a profile database;

in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair;

in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction;

if so determined, storing a digitally signed record of the payment transaction in a transaction archive; and

sending an authentication response to the seller over the network.

Claim 36 (previously presented) The method of claim 35, further comprising:

creating the PKI key pair; and

sending the private key to the buyer over the network.

Claim 37 (previously presented) The method of claim 35, wherein the record of the payment transaction is digitally signed using the private key.

Claim 38 (previously presented) The method of claim 35, wherein the record of the online transaction is digitally signed using a local private key.

Claim 39 (previously presented) The method of claim 35, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

Claim 40 (previously presented) The method of claim 35, further comprising:

retrieving a buyer profile from the database, the buyer profile including a plurality of payment instruments and a plurality of shipping addresses;

sending the buyer profile to the buyer over the network; and

receiving a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

Claim 41 (previously presented) The method of claim 35, further comprising:

processing the payment transaction via a payment gateway.

Claim 42 (previously presented) A computer readable medium storing instructions adapted to be executed by a processor, the instructions including a method for authenticating a payment transaction over a network, the method comprising:

storing a public key associated with a public key infrastructure (PKI) key pair in a profile database;

in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair;

in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction;

if so determined, storing a digitally signed record of the payment transaction in a transaction archive; and

sending an authentication response to the seller over the network.

Claim 43 (previously presented) The computer readable medium of claim 42, wherein the method further comprises:

creating the PKI key pair; and

sending the private key to the buyer over the network.

Claim 44 (previously presented) The computer readable medium of claim 42, wherein the record of the payment transaction is digitally signed using the private key.

Claim 45 (previously presented) The computer readable medium of claim 42, wherein the record of the online transaction is digitally signed using a local private key.

Claim 46 (previously presented) The computer readable medium of claim 42, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

Claim 47 (previously presented) The computer readable medium of claim 42, wherein the method further comprises:

retrieving a buyer profile from the database, the buyer profile including a plurality of payment instruments and a plurality of shipping addresses;

sending the buyer profile to the buyer over the network; and

receiving a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

Claim 48 (previously presented) The computer readable medium of claim 42, wherein the method further comprises:

processing the payment transaction via a payment gateway.

Claim 49 (previously presented) A system for authenticating a payment transaction over a network, comprising:

a profile database;

a transaction archive; and

an authentication service web server coupled to the profile database, the transaction archive and the network, the authentication service web server adaptively configured to:

store a public key associated with a public key infrastructure (PKI) key pair in a profile database;

in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, send a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair;

in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determine whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction;

if so determined, store a digitally signed record of the payment transaction in a transaction archive; and

send an authentication response to the seller over the network.

Claim 50 (previously presented) The system of claim 49, wherein the authentication service web server is further adapted to:

create the PKI key pair; and

send the private key to the buyer over the network.

Claim 51 (previously presented) The system of claim 49, wherein the record of the payment transaction is digitally signed using the private key.

Claim 52 (previously presented) The system of claim 49, wherein the record of the online transaction is digitally signed using a local private key.

Claim 53 (previously presented) The system of claim 49, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

Claim 54 (previously presented) The system of claim 49, wherein the authentication service web server is further adapted to:

retrieve a buyer profile from the database, the buyer profile including a plurality of payment instruments and a plurality of shipping addresses;

send the buyer profile to the buyer over the network; and

receive a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

Claim 55 (previously presented) The system of claim 49, wherein the authentication service web server is further adapted to:

process the payment transaction via a payment gateway.